ENGLISH TRANSLATION OF THE APPLICATION

4/PRTS

99P6221

Signing and signature checking of messages

A

FIELD OF THE INVENTION

~~Technical field~~

The invention relates to the signing and signature checking of messages using secret keys.

A

BACKGROUND OF THE INVENTION

~~Prior art~~

In order to provide protection against corruption of messages, it is known for symmetrical cryptography to be used to form a signature by means of which the receiver can check, with very high probability, whether the message has been transmitted without corruption and originates from the predetermined sender. However, one precondition is that the sender and receiver have a common, secret key, which must be stored in secure form. One such method is described, for example, in Patent Specification US 4,549,075.

Symmetrical cryptography, in particular the DES method, is frequently used in smart cards, because this method can be programmed very efficiently. The smart cards furthermore have a read only memory in which a main key is stored in secure and secret form, and this main key is also stored in secure form in a control center.

If it is now intended to send a message, protected against corruption, from a sender to the receiver, in this case the smart card, then, until now, the sender has had to have the message signed by the control center, since the control center cannot provide the sender with the secret main key

without weakening the entire system. Furthermore, measures are required to ensure that the message is protected against corruption and imitation of a legitimate sender during transmission from the sender to the main center.

The object of the invention is thus to specify a method for corruption protection of messages by means of a signature which can be formed by a sender and can be sent to a receiver without the sender having the secret main key, which is shared by the receiver and a control center, or without the message having to be sent in advance to the control center, for signature formation.

SUMMARY OF THE INVENTION

~~Description of the invention~~

The invention uses a method in which the control center forms signing keys in advance, and provides them to the sender. As is described in more detail in the exemplary embodiments, the receiver can model the signing key, and can thus check the message.

This relates to a method for signing a message, in which a control center and the receiver have a permanent, common main key. The control center produces a sequence number in advance, and produces a signing key from this by means of a one-time function. Both are provided to the sender, in secure form. The sender uses the signing key to form a signature for the message, and sends this signature with the sequence number and the message to the receiver. The receiver uses a one-time function, main key and sequence number to form a check key, and thus checks the signature on the message.

Further features and advantages of the invention result from the following description, which explains the invention with reference to an exemplary embodiment and in conjunction with the attached drawing.

Brief description of the drawing

In the figures:

Figure 1 shows a diagram in which the data flow is symbolized, with the components involved.

INS A17

~~Description of at least one embodiment at least of the invention~~

Figure 1 indicates the three parties involved in the method, namely the control center 10, the sender 20 and the receiver 30, separated by dashed-dotted lines.

The control center 10 contains a secure memory 11 for a secret key which is otherwise used, for example, in a symmetrical cryptographic encryption or signing method. The receiver 30 contains a corresponding memory 11', which contains the same key. This key is written to the control center during initialization, for example, if the receiver 30 is a smart card. Otherwise, key distribution methods known from cryptography can be used. In this case, the key is stored only once or at very long time intervals; the storage can be regarded as being permanent for the method according to the invention.

The control center 10 furthermore contains a sequence generator 12. This provides a series of numbers, which each differ. In the simplest case, this is a sequential number. However, it is better to use a known pseudo-random number generator, for example using the modulo method. If the parameters are chosen correctly, these pseudo-random number generators produce a sequence of new numbers in each case until the cycle which is governed by the modulus has been run through. Decreasing numbers or numbers with a step interval greater than unity can also be used. It is likewise possible to use the date and time as a unique sequence number, possibly as the number of seconds since an appointed start.

The control center thus produces one or more sequence numbers 12. A one-time encrypter 13 uses the main key to form a signing key 14 from such a sequence number 12. This is most easily done by the sequence number 12 being encrypted by means of the main key. In this case, a short sequence number is filled out by means of further data to the block length of the encryption method. Although binary zeros can be used for this purpose, it is better to use a function of the sequence number, for example its square. It is also possible to use a constant text, which does not consist of binary zeros and is kept confidential. Since the block size is generally in the same order of magnitude as the key length, it is still possible to use the result as a key; if necessary, bits must be added or the number of bits reduced by convolution.

The essential characteristic of the one-time encrypter is that it is virtually impossible to deduce the main

key. Although the method just described is not a one-time encryption since, for example, the receiver could form the sequence number from the signing key by decryption, the "one-time" functionality is the main feature.

Other one-time functions are thus used in other embodiments which link the main key and the sequence number in a reproducible manner to form a signing key without anyone who does not have the main key relating to a given sequence number being able to form a valid signing key, or vice versa, or being able to determine the main key from the signing key and the sequence number. Such methods are generally referred to as "message authentication codes" (MAC). One such method may be formed, in particular, by applying any desired cryptographically secure one-time function to a combination of a main key and sequence number. A concatenation, exclusive-OR, multiplication with or without modulo formation or addition, etc., may be used as the combination.

The control center 10 thus provides one or more pairs of sequence numbers 12, and signing keys 14 produced from them. This can be done, for example, by printing out on security paper, by storage in a further smart card or by some other secure data transmission. These pairs are provided to the sender 20 in advance, who must store them in a secure and confidential manner.

The sender 20 who wishes to send a message 21 to the receiver 30 takes a pair of sequence numbers 12 and signing keys 14 and uses the signer 24 to determine the signature for the message 21. The DES method, for example

in accordance with ANSI X9.9, is preferably also used in this case. Alternatively, a signature can be produced by a combination of a cryptographic hash function and a message authentication code. Methods relating to this have been described frequently and comprehensively in the cryptographic literature.

The sender then forms a data set 22, which contains three fields with the sequence number 22a, the message 22b and the signature 22c. The signing key 14 which has just been used is deleted.

The data set 22 is now transmitted to the receiver 30, which thus receives a data set 22' which once again contains three fields, which are regarded as the sequence number 22a', the message 22b' and the signature 22c'. Normally, this data set has already been protected against transmission errors by other security or plausibility mechanisms.

The receiver extracts the sequence number 22a' from the received data set 22', and passes this together with the main key 11' to one-time encryption 13' which, in the same way as the one-time encryption 13, is located in the control center 10 and is functionally identical to it. A check key 14' is produced at the output of the one-time function. If the sequence number has been transmitted correctly, this check key 14' is identical to the signing key 14 which the sender 20 has used. The check key 14' is passed to a signature checker 38 together with the message 22b' which has arrived and the signature 22c' which has arrived. If all three match one another, an enable signal for further use of the message is produced at the output of the signature checker 38. At the end of the check, the check key 14' is destroyed, irrespective of the result.

In one development of the invention, the receiver maintains a list of already used sequence numbers, and rejects messages with already used sequence numbers. This provides additional security against misuse.

Since the sequence number is preferably produced by a deterministic generator, there is no need to transmit the sequence number. Since the common main key has to be transmitted in a secure environment to the receiver in any case, the initial value of the generator can be transmitted at the same time. Whenever a message is received, the receiver produces a new value for the sequence number, and thus forms the check key 14' without the sequence number having to be transmitted as well. In order to be robust against double transmissions and lost messages, one of the last and following sequence numbers is expediently also then used. In this case as well, the control center can provide the sender with a number of signing keys 14, which the sender should then use in the predetermined sequence.

One possible application of the invention is in the field of automatic cash dispensers. The control center is in this case the bank control center, which uses a main key for checking the PIN and supplies personalized checking modules to the manufacturer of automatic cash dispensers in the control center. The sender may be a manufacturer or a local bank organization which, for example, wishes to load a currency conversion rate or a discount rate into the automatic cash dispensers; however, such organizations cannot introduce their own secret key into the cash dispenser, nor do they wish to install their own security module.

If the receiver does not contain a non-volatile memory, the receiver can also produce the sequence numbers from the start and test the signature with each of them. The loss of security in this case is low, but this does not provide any protection against double use.